Finite Fields and Their Applications 15 (2009) 82–96

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On complete (N, d)-arcs derived from plane curves

Herivelto Borges

Department of Mathematics, University of Texas at Austin, Austin, TX 78712, USA

ARTICLE INFO

Article history:
Received 3 May 2008
Revised 15 August 2008
Available online 18 September 2008
Communicated by Gary L. Mullen

Keywords:
Arcs
Complete (k, n)-arcs
Complete (N, d)-arcs
Fermat curves

ABSTRACT

In this paper, we present several new complete (N, d)-arcs obtained from $\mathbb{F}_q$-rational points of plane curves.

Published by Elsevier Inc.

0. Introduction

An (N, d)-arc $\mathcal{A}$ in the projective plane $PG(2, q)$ is a set of N points with at most d points on any line and with d points on some line. The (N, d)-arc is called complete if it is not contained in an $(N + 1, d)$-arc.

Natural examples of (N, d)-arcs are frequently obtained from a set $\mathcal{F}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of a plane curve $\mathcal{F}$ without linear components and defined over $\mathbb{F}_q$, where $N = \#\mathcal{F}(\mathbb{F}_q)$ and d is the degree of $\mathcal{F}$. One special motivation for studying such objects lies in its application to Coding Theory. Such (N, d)-arcs give rise to linear $[N, 3, N - d]$-codes over $\mathbb{F}_q$. If the underlying curve gives an (N, d)-arc, then the corresponding code has minimum distance $N - d$, and if it is complete, then it cannot be extended to a code with larger minimum distance.

Here, we will be mainly interested in (N, d)-arcs arising from plane curves. As a matter of terminology, we shall say that the curve $\mathcal{F}$ has the arc property whenever $\mathcal{F}$ gives rise to a complete $(\#\mathcal{F}(\mathbb{F}_q), d)$-arc in $PG(2, q)$. Deciding whether or not certain curves have the arc property is, in general, a difficult problem. With the exception of conics, cubics and Hermitian curves, very little is known about the arc property of curves in general. In Theorem 3.5 of [6], the authors give sufficient conditions for a Frobenius non-classical curve to have the arc property. They also present new complete arcs arising from plane curves, most having irreducible components given by $\mathbb{F}_q$-Frobenius

E-mail address: hbfilho@math.utexas.edu.

1071-5797/$ – see front matter Published by Elsevier Inc.
doi:10.1016/j.ffa.2008.08.003

non-classical curves. In contrast, our work here presents new complete arcs which are mostly derived from curves with $\mathbb{F}_q$-Frobenius classical components.

In [12], the authors constructed plane curves over $\mathbb{F}_p$, with the number of $\mathbb{F}_p$-rational points attaining the upper bound on Theorem 1.3. In [14], Voloch remarked that such curves would be somewhat large as (N,d)-arcs, and asked whether or not those (N,d)-arcs are complete.

In Section 2, after extending the construction of such curves to non-prime fields $\mathbb{F}_q$, we answer Voloch's question.

In Section 3, we consider a particular case of Theorem 1.4 and construct complete (N,d)-arcs of parameters $((q^2+4q-5)/4,(q-1)/2)$ and $((q^2+4q+7)/4,(q+3)/2)$ in $PG(2,q)$.

In Section 4, we intersect the Hermitian curve with certain conics, and prove that the $\mathbb{F}_{q^2}$-maximal curve $x^{\frac{q+1}{2}}+y^{\frac{q+1}{2}}+z^{\frac{q+1}{2}}=0$ gives rise to a complete $((q^3+3q+4)/4,(q+1)/2)$-arc in $PG(2,q^2)$. We also present complete $(q^3+q+2,q+3)$-arcs in $PG(2,q^2)$ by considering the union of the Hermitian curve with some conics.

In Section 5, we present a small complete (N,d)-arc of parameters $(2q-\sqrt{q}-1,\sqrt{q}-1)$ in $PG(2,q)$ obtained from another Fermat curve.

In Section 6, we have a table summarizing the (N,d)-arcs and compare some of our parameters with others previously obtained. The Griesmer bound is also discussed.

1. Preliminaries

This section introduces some concepts and results used throughout the next sections. In particular, we give a brief overview regarding $\mathbb{F}_q$-Frobenius (non-)classicality of plane curves and establish some combinatorial properties of a special set of lines in $PG(2,q)$. This set will turn out to be important in the development of Sections 2 and 3.

Let $\mathcal{F}$ be a non-singular projective curve of genus g defined over $\mathbb{F}_q$. If $N=\#\mathcal{F}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points of $\mathcal{F}$, then the famous Hasse–Weil theorem gives

$$\left|N-(q+1)\right|\leqslant 2gq^{1/2}. \tag{1.1}$$

There are many examples of curves $\mathcal{F}$ attaining the Hasse–Weil upper bound, i.e. $N=\mathcal{F}(\mathbb{F}_q)=1+q+2gq^{1/2}$. Because this can only happen if q is a square or $g=0$, such curves are usually called $\mathbb{F}_{q^2}$-maximal.

A very well-known example of an $\mathbb{F}_{q^2}$-maximal curve is the Hermitian curve

$$\mathcal{H}:\quad x^{q+1}+y^{q+1}+z^{q+1}=0$$

which is a non-singular plane curve of genus $\frac{1}{2}(q^2-q)$ with exactly $1+q^3$ points in $PG(2,q^2)$.

The Hermitian curve, together with its large automorphism group, gives rise to many other $\mathbb{F}_{q^2}$-maximal curves (see for example [4]). A very simple example of this is given by the following result.

Theorem 1.1. *If q is a prime power and d is a divisor of $q+1$, then the curve*

$$x^d+y^d+z^d=0$$

is $\mathbb{F}_{q^2}$-maximal.

The case $d=(q+1)/2$ in Theorem 1.1 will be considered in Section 4.

The next result (see for example [8, Chapter 7]), which will be used in the proof of Theorem 4.2, states another interesting property of the Hermitian curve.

Theorem 1.2. *Let $\mathcal{H}$ be the Hermitian curve, P a point in $PG(2,q^2)\setminus\mathcal{H}(\mathbb{F}_{q^2})$ and L_P the set of q^2+1 lines in $PG(2,q^2)$ incident with P. If $l\in L_P$ such that $\#(l\cap\mathcal{H}(\mathbb{F}_{q^2}))<q+1$, then $\#(l\cap\mathcal{H})=1$. Moreover, there are exactly $q+1$ such lines in L_P.*

Note that Theorem 1.2 implies $\mathcal{H}(\mathbb{F}_{q^2})$ is a complete $(q^3+1, q+1)$-arc in $PG(2, q^2)$. In Sections 4 and 5, the above properties of the Hermitian curve will be useful in obtaining other curves with the arc property.

In Section 2, we will deal with curves that have many points and do not meet the Hasse–Weil upper bound. To make this idea of many points clearer, we need to recall some of the improvements on the Hasse–Weil bound given by the work of Stöhr and Voloch in [13]. A very important ingredient in Stöhr–Voloch's approach is the notion of $\mathbb{F}_q$-Frobenius (non-)classical curve. In what follows, we present only concepts and facts that will be relevant to our context. In particular, we restrict our discussion to the case of plane curves.

Let $q = p^h$ be a prime power and $\mathcal{F}$ be an irreducible plane curve defined over $\mathbb{F}_q$. The curve $\mathcal{F}$ is called $\mathbb{F}_q$-Frobenius non-classical if the image P^q of each simple point P of $\mathcal{F}$ under the Frobenius map lies on the tangent line at P. Some of the properties of such curves can be found in [7]. For instance, for $p > 2$ an $\mathbb{F}_q$-Frobenius non-classical curve is the locus of its singular and inflection points. Also, with the additional hypothesis that $\mathcal{F}$ is smooth, Hefez and Voloch [7, Theorem 1] managed to prove that

$$\#\mathcal{F}(\mathbb{F}_q) = d(q - d + 2)$$

where d is the degree of $\mathcal{F}$.

Examples of $\mathbb{F}_q$-Frobenius non-classical curves are the Fermat curves

$$x^d + y^d + z^d = 0$$

where $d = \frac{q-1}{q'-1}$ and q' is a power of $p > 2$. We remark that such Fermat curves are part of the list of curves with the arc property[1] presented in [6]. Note that the Hermitian curve $\mathcal{H}$ also lies in this family.

If a curve $\mathcal{F}$ is $\mathbb{F}_q$-Frobenius classical, then an upper bound for $\#\mathcal{F}(\mathbb{F}_q)$, namely $d(d+q-1)/2$, can be obtained from Theorem 2.13 of [13]. However, for our purposes, it suffices to present only a simple case of that result (see [13, Theorem 0.1]):

Theorem 1.3. *Let q be an odd prime power. If $\mathcal{F} = Z(f(x, y))$ is an absolutely irreducible plane curve of degree d defined over $\mathbb{F}_q$, then*

$$\#\mathcal{F}(\mathbb{F}_q) \leqslant d(d+q-1)/2$$

provided that f does not divide $(f_y)^2 f_{xx} - 2 f_{xy} f_x f_y + (f_x)^2 f_{yy}$.

Note that the last condition in the theorem above only means that $\mathcal{F}$ has finitely many inflection points. This fact will be used in Section 2, where we present a family of curves meeting the upper bound above and investigate their arc property. In this investigation, a special set of lines will play an important role; some of the basic properties of such a set are presented next.

Theorem 1.4. *Let q be a prime power and k be a divisor of $q-1$. If L is the set of $3(k+1)$ lines in $PG(2, q)$ given by the components of $xyz(x^k - y^k)(x^k - z^k)(y^k - z^k) = 0$, then the number of points in $PG(2, q)$ comprised by the union of such lines is given by*

$$3q(k+1) - 3k - 2k^2. \tag{1.2}$$

[1] It should be noted that not all $\mathbb{F}_q$-Frobenius non-classical curves have the arc property. For an example, one can check the curve $x^{40} + y^{40} + z^{40} + (x+y+z)^{40} = 0$ over F_{81}.

In addition, if we define the sets

$$A = \left\{(\xi_i : \xi_j : 1) \;\middle|\; 1 \leqslant i, j \leqslant k \text{ and } \xi_i^k = \xi_j^k = 1\right\},$$

$$B = \left\{(\xi_i : 1 : 0), (\xi_i : 0 : 1), (0 : 1 : \xi_i) \;\middle|\; 1 \leqslant i \leqslant k \text{ and } \xi_i^k = 1\right\},$$

$$C = \left\{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)\right\},$$

then the following holds:

(1) *$A \cup B \cup C$ is the set of all points that occur as the intersection of lines in L.*
(2) *Each point in C lies on exactly $k + 2$ lines in L.*
(3) *Each point P in A lies on exactly three lines in L. These three lines are the ones connecting P with each point in C.*
(4) *Each point P in B lies on exactly two lines in L. One such line connects the two points of C collinear with P, and the other line connects P with the third point of C.*

Proof. Let L_1, L_2 and L_3 be the sets of lines corresponding to the linear components of $y^k - z^k = 0$, $x^k - z^k = 0$ and $x^k - y^k = 0$, respectively. It is clear that the k lines in each of the three sets are incident with a point in $C = \{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1)\}$. Therefore, the union of lines in each set L_i comprises $kq + 1$ points of $PG(2, q)$. Also, intersecting the lines from any two different sets L_i and L_j, gives us the same set of k^2 points, namely $A = \{(\xi_i : \xi_j : 1) \mid 1 \leqslant i, j \leqslant k \text{ and } \xi_i^k = \xi_j^k = 1\}$. Thus, by the inclusion–exclusion principle we have collected $3(kq + 1) - 2k^2$ points in $PG(2, q)$ comprised by the union of the lines in the sets L_i, $i = 1, 2, 3$. One can also see that the line $x = 0$ intersects the lines from L_1 in a set of k points, namely $\{(0 : 1 : \xi_i) \mid 1 \leqslant i \leqslant k \text{ and } \xi_i^k = 1\}$ and intersects the lines from L_2 and L_3 at $(0 : 1 : 0)$ and $(0 : 0 : 1)$, respectively. Thus, including the line $x = 0$ will only give us $(q + 1) - (k + 2) = q - k - 1$ extra points. By symmetry, including the three components of $xyz = 0$ will give us $3(q - k - 1)$ extra points. Therefore, the union of the $3(k + 1)$ lines of L will provide a set of $3(kq + 1) - 2k^2 + 3(q - k - 1) = 3q(k + 1) - 3k - 2k^2$ points in $PG(2, q)$. Finally, one should note that the counting process above automatically reveals the properties claimed for the sets A, B and C. □

Corollary 1.5. *If $S \subset PG(2, q)$ is the set of points comprised by the union of the $3(k + 1)$ lines in L, and l is a line in $PG(2, q)$ which is not in L, then the following holds*:

(1) *$S = PG(2, q)$ if and only if $k = (q - 1)/2$ or $k = q - 1$.*
(2) *If $\#(l \cap C) > 0$, then $\#(l \cap A) = \#(l \cap B) = 0$ and $\#(l \cap S) = 2k + 2$.*
(3) *If $\#(l \cap C) = 0$, then $\#(l \cap S) = 3(k + 1) - (2\#(l \cap A) + \#(l \cap B))$.*

Proof. (1) This follows directly from $\#S = 3q(k + 1) - 3k - 2k^2$.

(2) We may assume $l \cap C = \{(1 : 0 : 0)\}$, with l given by $y - \alpha z = 0$ and $\alpha \neq 0$. It is clear that if we have either $\#(l \cap A) > 0$ or $\#(l \cap B) > 0$, then we get $\alpha^k = 1$ which implies $l \in L$, a contradiction. Therefore, $\#(l \cap A) = \#(l \cap B) = 0$. Now, by Theorem 1.4(2), l intersects $k + 2$ lines in L at $P = (1 : 0 : 0)$, and, by Theorem 1.4(1), l intersects the remaining $2k + 1$ lines at $2k + 1$ distinct points. That gives $\#(l \cap S) = 2k + 2$.

(3) Since $l \notin L$, items (3) and (4) of Theorem 1.4 imply that, for each $P \in l \cap A$, l intersects three lines in L meeting at P, and for each $Q \in l \cap B$, l intersects two lines of L meeting at Q. Therefore l intersects $3\#(l \cap A) + 2\#(l \cap B)$ lines in L in a set of $\#(l \cap A) + \#(l \cap B)$ points. Since $\#(l \cap C) = 0$, Theorem 1.4(1) implies that l intersects the remaining $3(k+1) - (3\#(l \cap A) + 2\#(l \cap B))$ lines in exactly $3(k + 1) - (3\#(l \cap A) + 2\#(l \cap B))$ points. Hence, $\#(l \cap S) = 3(k + 1) - (2\#(l \cap A) + \#(l \cap B))$. □

2. Arcs obtained from curves with many points

A construction of curves (over $\mathbb{F}_p$) attaining the upper bound in Theorem 1.3 is presented in [12]. Here, we present the corresponding construction over non-prime fields $\mathbb{F}_q$, and referring to such curves as "$\mathcal{C}_k$," we investigate $\mathcal{C}_k(\mathbb{F}_q)$ viewed as (N,d)-arcs.

Theorem 2.1. *Let $q=p^u$ be an odd prime power and $k<(q-1)/2$ be a divisor of $q-1$ such that $p\nmid(k+1)$. If $m=\frac{q-1-2k}{k}$, then the plane curve*

$$\mathcal{C}_k\colon \sum_{r+s+t=m}\left(x^r y^s z^t\right)^k=0$$

is smooth of degree $d=q-1-2k$, and $\#\mathcal{C}_k(\mathbb{F}_q)=d(d+q-1)/2$.

Proof. Defining $h(t)=(t^{q-1}-1)/(t^k-1)$, we can see that $f(x,y)=(h(x)-h(y))/(x^k-y^k)$ is a polynomial of degree $d=q-1-2k$. Also, since $d=mk$, one can check that $z^d f(\frac{x}{z},\frac{y}{z})=\sum_{r+s+t=m}(x^r y^s z^t)^k$.

The smoothness part can be derived from the fact that $f(x,y)=G_m(x^k,y^k,1)$, where $G_m(x,y,z)=0$ is the curve in Theorem 1 of [12], which is smooth whenever $p\nmid(m+1)(m+2)$.

To count the $\mathbb{F}_q$-solutions of $f(x,y)=0$, note that $h(\alpha)=h(\beta)=0$ with $\alpha^k\neq\beta^k$ implies $f(\alpha,\beta)=0$. Therefore, all the pairs $(\alpha,\beta)\in\mathbb{F}_q\times\mathbb{F}_q$ satisfying $1\neq\alpha^k\neq\beta^k\neq 1$ and $\alpha\beta\neq 0$ will be solutions of $f(x,y)=0$. Since $k(m+2)=q-1$, the $m+1$ choices of α^k followed by the m choices of β^k give $(m+1)mk^2=d(d+q-1)/2$ such solutions.

To show that $\mathcal{C}_k$ is attaining the upper bound in Theorem 1.3, it suffices to prove that $\mathcal{C}_k$ has finitely many inflection points. This is indeed the case because $p\nmid(d-1)$, and we can apply Corollary 2.2 of [11]. Hence, $\#\mathcal{C}_k(\mathbb{F}_q)=d(d+q-1)/2$. □

We point out that because the upper bound was achieved, $f(x,y)=0$ has no solution $(\alpha,\beta)\in\mathbb{F}_q\times\mathbb{F}_q$ with either coordinate being zero or a kth root of unity. An immediate consequence is that the $3(k+1)$ lines given by the components of $xyz(x^k-y^k)(x^k-z^k)(y^k-z^k)=0$ do not intersect $\mathcal{C}_k(\mathbb{F}_q)$. This fact will be used later in Proposition 2.3.

The next theorem is the main result of this section.

Theorem 2.2. *Let $q=p^m$ be a prime power, $p>5$, and let $k<(q-1)/2$ be a divisor of $q-1$. If N is the number of $\mathbb{F}_q$-rational points and d is the degree of the curve $\mathcal{C}_k$, then $\mathcal{C}_k(\mathbb{F}_q)$ is a complete (N,d)-arc if and only if $k=1,2,4,6,(p^r-1)/2$ or $2(p^r-1)$, where $r\mid m$, $r<m$ and m/r is assumed to be even in the last case. Moreover, if $k=3\neq(p-1)/2$, then one can always adjoin exactly 9 points and have a complete $(q^2-11q+37,q-7)$-arc.*

The proof of this theorem will be given through a sequence of several partial results. The first partial result provides a very useful way of seeing the $\mathbb{F}_q$-rational points of the curves $\mathcal{C}_k$.

Proposition 2.3. *The set of $\mathbb{F}_q$-rational points of a curve $\mathcal{C}_k$ is the complement, in $PG(2,q)$, of the union of the $3(k+1)$ lines given by the components of $xyz(x^k-y^k)(x^k-z^k)(y^k-z^k)=0$.*

Proof. Note that we have the same set L of the $3(k+1)$ lines of Theorem 1.4 and $\#(l\cap\mathcal{C}_k(\mathbb{F}_q))=0$ for each line $l\in L$. Now, using (1.2) and

$$3q(k+1)-3k-2k^2+\#\mathcal{C}_k(\mathbb{F}_q)=1+q+q^2,$$

we get the result. □

We will stick to the notation used in Theorem 1.4 and Corollary 1.5 for the remaining of this section. The sets A, B, C, L and S will be used throughout, and the points in the sets A, B and C will be often referred to as A-points, B-points and C-points, respectively. Also, for future purposes, the following remark (based on Proposition 2.3) should be kept in mind:

Remark 2.4. For any line l of $PG(2,q)$, since $d = q-1-2k$, we have $\#(l \cap S) \geqslant 2k+2$. Equality holds if and only if $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$.

Now, if $N = \#\mathcal{C}_k(\mathbb{F}_q)$ and d is the degree of $\mathcal{C}_k$, the next result shows that $\mathcal{C}_k(\mathbb{F}_q)$ is indeed an (N,d)-arc. In addition, we will also see that the check for the arc property can later be restricted to the points of $A \cup B$. Recall that A, B and C are given in Theorem 1.4.

Proposition 2.5. *If $P \in PG(2,q)$ is a point in the complement of $\mathcal{C}_k(\mathbb{F}_q)$ such that $P \notin A \cup B$, then there exists a line l containing P such that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$.*

Proof. Since $P \notin A \cup B$ by Theorem 1.4 we can pick a line $l \notin L$ containing P and a point in C. Since $\#(l \cap C) > 0$, Corollary 1.5(2) gives $\#(l \cap S) = 2k+2$. Now, Remark 2.4 completes the proof. □

Later on, we will notice that there is a set of Fermat curves associated with each curve $\mathcal{C}_k$. It turns out that requiring our (N,d)-arcs to be complete is nearly equivalent to requiring such Fermat curves to have "many" $\mathbb{F}_q$-rational points. Considering this, we will first recall some results regarding upper bounds on the number of $\mathbb{F}_q$-rational points on Fermat curves.

The following lemma is a consequence of inequality $(4')$ and Theorem 3 of [5].

Lemma 2.6. *Let $\mathbb{F}_{p^m}$ be a finite field of characteristic $p > 5$, and $n > 2$ be a divisor of $p^m - 1$ not satisfying any of the following conditions*:

(i) $p \mid (n-1)$.
(ii) $n = 2(p^m-1)/(p^r-1)$ *for some divisor r of m, with $r < m$.*
(iii) $n = (p^m-1)/2(p^r-1)$ *for some divisor r of m, where m/r is an even number.*

If $q = p^m$ and $a, b \in \mathbb{F}_q^\star$, then the number $N_n(a,b,q)$ of $\mathbb{F}_q$-rational points of the Fermat curve $ax^n + by^n + z^n = 0$ satisfies

$$N_n(a,b,q) \leqslant n^2 \left\lfloor \frac{2(q-1+2n-\delta)}{5n} \right\rfloor + \delta$$

where δ is the number of such points with $xyz = 0$.

Lemma 2.7. *Let $q = p^m$ be a prime power, $p > 5$, and k a divisor of $q-1$ such that $n = (q-1)/k$ satisfies the same hypotheses as in the previous lemma. If l is a line given by $ax + by + z = 0$ with $a, b \in \mathbb{F}_q^\star$, then the following holds*:

(1) *l contains at most $\lfloor \frac{2(k+2-\epsilon(l))}{5} \rfloor$ A-points, where $\epsilon(l)$ is the number of B-points on l;*
(2) *for $p > 7$, if $k = 3$ and $\epsilon(l) \geqslant 2$, then l does not contain an A-point;*
(3) *for $k = 5$, if $\epsilon(l) \geqslant 2$, then l contains at most one A-point.*

Proof. (1) This follows directly from Lemma 2.6.

Note that the last two statements do not follow from the first one. Also, $\epsilon(l) \in \{0,1,2,3\}$ for every line l.

(2) Suppose we have two B-points of l given by $(0:1:-b)$ and $(1:0:-a)$. It follows that $-a$ and $-b$ are cubic roots of unity and therefore the line l can be given by $x + y = z$. If l contains an A-point, then the equation $x + y = 1$ has a solution for x and y in $\{1, \omega, \omega^2\}$, the cubic roots of unity. Since

$1+\omega+\omega^2=0$, we clearly see there is no solution for $x\neq y$. On the other hand, a solution for $2x=1$ implies $p=7$, contradicting one hypothesis.

If the B-points are not the ones we considered, we may assume they are given by $(0:1:-b)$ and $(1:-a/b:0)$. This implies that a and $-b$ are cubic roots of unity, and the line equation may be given by $x+z=y$. The result then follows from an equivalent argument given in the previous case.

(3) Again, suppose l contains the B-points given by $(0:1:-b)$ and $(1:0:-a)$. It follows that $-a$ and $-b$ are fifth roots of unity, and the equation of l can be given by $x+y=z$. If l contains two A-points, then the equation $x+y=1$ has two solutions for x and y in $\{1,\omega_1,\ldots,\omega_4\}$, the fifth roots of unity. It is clear that we have $x\neq 1\neq y$. If $x\neq y$ for both solutions, then we may assume the two solutions are given by $\omega_1+\omega_2=1$ and $\omega_3+\omega_4=1$. This implies $\omega_1+\omega_2+\omega_3+\omega_4=2$ and then $p=3\leqslant 5$, a contradiction. If we have a solution with $x=y$, then we get $2x=1$, which implies $p=31$. However, the fifth roots of unity for this case are given by $\{1,2,4,8,16\}$, and there is no way we can have a second distinct solution. Similarly to the previous case, for a different choice of B-points, we get an equivalent situation, and again the result follows. □

In the next two results, k satisfies the hypotheses of Lemma 2.7. We also recall that N and d will stand for the number of $\mathbb{F}_q$-rational points and the degree of the curve $\mathcal{C}_k$, respectively.

Lemma 2.8. *For $k>6$, $\mathcal{C}_k(\mathbb{F}_q)$ is not a complete (N,d)-arc.*

Proof. We will argue by contradiction. Let P be an A-point and l a line containing P such that $\#(l\cap\mathcal{C}_k(\mathbb{F}_q))=d$. If l contains m A-points and $\epsilon(l)$ B-points, then by Corollary 1.5(3) we have $\#(l\cap S)=3k+3-2m-\epsilon(l)$ points. By Remark 2.4, we have $3k+3-2m-\epsilon(l)=2k+2$, which gives $m=(k+1-\epsilon(l))/2$. Now, from Lemma 2.7(1), we have $(k+1-\epsilon(l))/2\leqslant 2(k+2-\epsilon(l))/5$ which gives $k\leqslant\epsilon(l)+3\leqslant 6$. □

Lemma 2.9. *If $k=3$ or $k=5$, then $\mathcal{C}_k(\mathbb{F}_q)$ is not a complete (N,d)-arc. However, in the first case, we can always adjoin 9 points to $\mathcal{C}_k(\mathbb{F}_q)$ and obtain a complete $(q^2-11q+37,q-7)$-arc.*

Proof. (i) Case $k=3$. Note this implies $p>7$. In fact, if $p=7$, we have $k=(p-1)/2$, violating our hypotheses on k. Assume the arc is complete. Let P be a B-point, and suppose l is a line through P such that $\#(l\cap\mathcal{C}_k(\mathbb{F}_q))=d$. Since $\epsilon(l)\geqslant 1$, by Lemma 2.7(1), l contains at most one A-point. If the number of A-points is zero, then Corollary 1.5(3) gives $\#(l\cap S)\geqslant 3(k+1)-3=9>2k+2$. If l contains one A-point, then by Lemma 2.7(2) the line contains only one B-point and then $\#(l\cap S)=3(k+1)-2-1=9>2k+2$. Both cases contradict Remark 2.4. Hence, the arc is not complete. On the other hand, one can easily check that any line $l\notin L$ connecting two A-points satisfies $\#(l\cap\mathcal{C}_k(\mathbb{F}_q))=d$. Since by Lemma 2.7(1) such a line does not contain a B-point, we can use Lemma 2.7(2) to include all 9 B-points into our set without having $d+1$ collinear points. That will finally give us a complete $(q^2-11q+37,q-7)$-arc.

(ii) Case $k=5$. Again we suppose the arc is complete and take a line l containing an A-point P and satisfying $\#(l\cap\mathcal{C}_k(\mathbb{F}_q))=d$. If $\epsilon(l)\geqslant 2$, then by Lemma 2.7(3) l contains only one A-point, which implies $\#(l\cap S)\geqslant 3(k+1)-2-3=13>2k+2$. If $\epsilon(l)\leqslant 1$, then Lemma 2.7(1) states l contains at most two A-points, and we have $\#(l\cap S)\geqslant 3(k+1)-4-1=13>2k+2$. In either case, we contradict Remark 2.4. Therefore, the arc is not complete. □

Next, we will prove that we have complete (N,d)-arcs in the remaining cases.

Lemma 2.10. *If there exists a line l in $PG(2,q)$ connecting an A-point to a B-point such that $\#(l\cap\mathcal{C}_k(\mathbb{F}_q))=d$, then $\mathcal{C}_k(\mathbb{F}_q)$ is a complete (N,d)-arc.*

Proof. This follows directly from the fact that $H\cong(\mathbb{Z}/k\mathbb{Z})^2\rtimes S_3$ is a subgroup of $\mathrm{Aut}(\mathcal{C}_k)$, and H acts transitively on the sets A and B. □

Proposition 2.11. *Let $p > 5$ be a prime and m and r be positive integers such that $m > r$ and $r \mid m$.*

1. *If m/r is even and $k = 2(p^r - 1)$, then the line l: $x + y + z = 0$ contains exactly $p^r - 2$ A-points and three B-points defined over $\mathbb{F}_{p^m}$.*
2. *Let $\chi_{p^r}\colon \mathbb{F}_{p^r}^{\times} \to \{\pm 1\}$ be the quadratic character, and consider the line l: $x + \chi_{p^r}(-1)y = z$. For $k = (p^r - 1)/2$, the line l contains exactly $(p^r - 5)/4$ A-points and three B-points if $\chi_{p^r}(-1) = 1$, and l contains exactly $(p^r - 3)/4$ A-points and two B-points if $\chi_{p^r}(-1) = -1$. Such points are also defined over $\mathbb{F}_{p^m}$.*

Proof. The statements follow directly from the computation of the number of $\mathbb{F}_{p^m}$-rational points on the curves $ax^{e/2} + by^{e/2} + z^{e/2} = 0$ (with $a^2, b^2 \in \mathbb{F}_{p^r}$) and $ax^{2e} + by^{2e} + z^{2e} = 0$ (with $a, b \in \mathbb{F}_{p^r}$), where $e = (p^m - 1)/(p^r - 1)$. For such computation, see Examples (vii) and (viii) of [5]. □

The proof of Theorem 2.2 is completed by the following lemma.

Lemma 2.12. *If $k = 1, 2, 4, 6, (p^r - 1)/2$ or $2(p^r - 1)$, then $\mathcal{C}_k(\mathbb{F}_q)$ are complete (N, d)-arcs. In particular, using the two last values of k and $q = p^m$, we prove the existence in $PG(2, q)$ of a complete*

$$\left(\frac{2q^2 - (3p^r + 1)q + p^{2r} + p^r}{2}, q - p^r\right)\text{-arc}, \quad \text{where } r \mid m \text{ and } r < m, \tag{2.1}$$

and a complete

$$\left(q^2 + \left(4 - 6p^r\right)q + 8p^{2r} - 10p^r + 3, q - 4p^r + 3\right)\text{-arc}, \quad \text{where } r \mid m \text{ and } \frac{m}{r} \text{ is even.} \tag{2.2}$$

Proof. For each given k, it suffices to find a line l fulfilling the conditions of Lemma 2.10.

- Case $k = 2(p^r - 1)$: We consider the line l: $x + y + z = 0$. By Proposition 2.11, l contains $p^r - 2$ A-points and $\epsilon(l) = 3$. Thus, using Corollary 1.5(3), one can check that $\#(l \cap S) = 2k + 2$. Therefore, by Remark 2.4, we have $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$, and Lemma 2.10 completes the proof.
- Case $k = (p^r - 1)/2$: We take the line l: $x + \chi_{p^r}(-1)y = z$ from Proposition 2.11, and similar to the previous case, one can check that $\#(l \cap \mathcal{C}_k(\mathbb{F}_q)) = d$ and the result follows.
- Case $k = 6$: Let $\{\pm 1, \pm\omega, \pm\omega^2\}$ be the set of the sixth roots of unity. It is clear that the line l: $\omega x + \omega^2 y + z = 0$ contains the A-points $P = (1 : 1 : 1)$, $Q = (\omega : \omega^2 : 1)$ and the B-points $(-\omega : 1 : 0), (-\omega^2 : 0 : 1), (0 : -\omega : 1)$. The usual check shows that $\#(l \cap S) = 14 = 2k + 2$, and the result follows again. The cases $k = 1, 2$ and 4 can be handled in a similar (or even simpler) way. □

3. Arcs of parameters $((q^2 + 4q - 5)/4, (q - 1)/2)$ and $((q^2 + 4q + 7)/4, (q + 3)/2)$ in $PG(2, q)$

In the previous section, we considered the (N, d)-arcs in $PG(2, q)$ given by the complement of the union of the $3(k + 1)$ lines in L. Now, we will be interested in the case where such a complement is empty, i.e., the set S is the whole $PG(2, q)$. By Corollary 1.5(1), this happens if and only if $k = q - 1$ or $k = (q - 1)/2$. We will consider the case where $k = (q - 1)/2$ and use the sets A, B and C to construct complete (N, d)-arcs. The same can be done in the case $k = q - 1$, but we will get either the trivial complete $(1 + q + q^2, q + 1)$-arc or the complete $((q - 1)^2, q - 1)$-arc arising from the curve $x^{q-1} + y^{q-1} = 2z^{q-1}$, which was already considered in [6].

Theorem 3.1. *Let $q > 11$ be an odd prime power. If Γ is the curve given by $(x^k + y^k - 2z^k)(x^k + z^k - 2y^k)(y^k + z^k - 2x^k) = 0$ where $k = (q - 1)/2$, then $\Gamma(\mathbb{F}_q)$ is a complete $((q^2 + 4q - 5)/4, (q - 1)/2)$-arc.*

Proof. Let $\mathcal{F}$ be the curve given by $x^k + y^k - 2z^k = 0$. It is easy to check that $\mathcal{F}(\mathbb{F}_q) = A \cup \{(\xi_i : 1 : 0)\colon\ \xi_i^k = -1\}$, where A is given as in Theorem 1.4. Therefore, by symmetry, we have $\#\Gamma(\mathbb{F}_q) = k^2 + 3k = (q^2 + 4q - 5)/4$. It is clear that we have k collinear points in $\Gamma(\mathbb{F}_q)$, and we now suppose the existence of a line incident with $k + 1$ points of this set. Note that $\Gamma(\mathbb{F}_q) \setminus A$ is a subset of the lines given by the components of $xyz = 0$. So, any line containing $k + 1$ points of $\Gamma(\mathbb{F}_q)$ would take at most three points from this subset and at least $k - 2$ points from A. Suppose $l\colon ax + by + cz = 0$ is such a line. If $abc = 0$, then it is easy to check that l is a line in L intersecting $\Gamma(\mathbb{F}_q)$ in exactly k points. Therefore, we may assume l is given by $ax + by + z = 0$, and $ab \neq 0$. On the other hand, such a condition implies that each A-point in l gives rise to four affine points on the conic $ax^2 + by^2 + z^2 = 0$. This fact yields $4(k - 2) \leqslant q + 1$ and thus $q \leqslant 11$, a contradiction. Therefore $\Gamma(\mathbb{F}_q)$ is a $((q^2 + 4q - 5)/4, (q - 1)/2)$-arc. The arc property follows from the fact that $PG(2, q)$ is covered by the $3(k + 1)$ lines of L and that $\Gamma(\mathbb{F}_q)$ has k points on each one of those lines. □

With a similar reasoning using the sets A, B and C, the next result presents another complete (N, d)-arc. However, unlike Theorem 3.1, the underlying set is not apparently given by the $\mathbb{F}_q$-rational points of a curve.

Theorem 3.2. *Let q be an odd prime power and $k = (q - 1)/2$. If $W = \{(x_0 : x_1 : x_2) \in PG(2, q) \mid x_i^k \in \{0, 1\}\}$, then W is a complete $((q^2 + 4q + 7)/4, (q + 3)/2)$-arc.*

Proof. It is clear that $W = A \cup B \cup C$ and $\#W = k^2 + 3k + 3 = (q^2 + 4q + 7)/4$. Note that each of the $3(k+1)$ lines of L is incident with $k+2 = (q+3)/2$ points of W. Suppose we have $(q+3)/2+1 = k+3$ points in W incident with a line $l\colon ax + by + cz = 0$, $l \notin L$. Observe that $B \cup C$ is a subset of the union of lines given by $xyz = 0$ and A is a subset of the $\mathbb{F}_q$-rational points of $x^k + y^k - 2z^k = 0$. Therefore, l must be incident with three points in $B \cup C$ and k points in A. Now, from an argument similar to the one used in the proof of the previous theorem, we conclude $4k \leqslant q + 1$ and thus $q \leqslant 3$. On the other hand, one can easily check that such a line does not exist for $q = 3$. Therefore, W is a $((q^2 + 4q + 7)/4, (q + 3)/2)$-arc. Completeness also follows similarly to Theorem 3.1. □

4. An $\mathbb{F}_{q^2}$-maximal curve

Recall from Theorem 1.1 that for any divisor d of $q + 1$ the curve $x^d + y^d + z^d = 0$ is $\mathbb{F}_{q^2}$-maximal. Given that such curves are somewhat large as (N, d)-arcs, it is natural to ask about their arc property. Among these curves, we consider a special one given by

$$x^{(q+1)/2} + y^{(q+1)/2} + z^{(q+1)/2} = 0 \tag{4.1}$$

which is the unique (up to $\mathbb{F}_{q^2}$-isomorphism) smooth $\mathbb{F}_{q^2}$-maximal plane curve of such degree, provided that $q \geqslant 11$ (see [3]).

In this section, after investigating the intersection of the Hermitian curve with certain conics, we prove the following:

Theorem 4.1. *Let q be an odd prime power. If Γ is the curve given by $x^{(q+1)/2} + y^{(q+1)/2} + z^{(q+1)/2} = 0$, then $\Gamma(\mathbb{F}_{q^2})$ is a complete $((q^3 + 3q + 4)/4, (q + 1)/2)$-arc.*

Theorem 4.2. *If $q > 3$ is an odd prime power, and $\mathcal{H}\colon x^{q+1} + y^{q+1} + z^{q+1} = 0$ is the Hermitian curve, then there exists a conic $\mathcal{C}$, defined over $\mathbb{F}_{q^2}$, such that $\mathcal{H}(\mathbb{F}_{q^2}) \cap \mathcal{C}(\mathbb{F}_{q^2}) = \emptyset$. Moreover, $\mathcal{H}(\mathbb{F}_{q^2}) \cup \mathcal{C}(\mathbb{F}_{q^2})$ gives rise to a complete $(q^3 + q^2 + 2, q + 3)$-arc in $PG(2, q^2)$.*

We proceed by presenting a list of preliminary results that will lead to the proof of both theorems. The following notation will be carried out for the rest of this paper.

For $i = 1, 2$, we set $N_i := \{\xi \in \mathbb{F}_{q^2}\colon\ \xi^{(q+1)/2} = (-1)^i\}$, and the quadratic character $\chi_{q^i} : \mathbb{F}_{q^i}^{\times} \mapsto \{\pm 1\}$. Note that $N = \{\xi \in \mathbb{F}_{q^2}\colon\ \xi^{q+1} = 1\} = N_1 \cup N_2$ and $N_2 = \{\xi^2\colon\ \xi \in N\}$.

Lemma 4.3. *If $\chi_{q^2}(r) = -1$, then $\{(r-\xi)^{q+1}\colon\ \xi \in N_1\} = \{(r-\xi)^{q+1}\colon\ \xi \in N_2\}$.*

Proof. For $\xi \in N_1$, the condition $\chi_{q^2}(r) = -1$ implies $\frac{1}{\xi r^{q-1}} \in N_2$. Now we have $(r-\xi)^{q+1} = (r-\xi)^{q(q+1)} = (r^q - \frac{1}{\xi})^{q+1} = (r^{q-1}(r - \frac{1}{\xi r^{q-1}}))^{q+1} = (r - \frac{1}{\xi r^{q-1}})^{q+1}$, from which we conclude that the two sets are the same. □

The following remark will be a useful tool in the proofs of the next results.

Remark 4.4. If $N = \{\xi \in \mathbb{F}_{q^2}\colon\ \xi^{q+1} = 1\}$ and $\epsilon \in \mathbb{F}_{q^2}$ is such that $\epsilon^{q-1} = -1$, then $N = \{\frac{t+\epsilon}{t-\epsilon}\colon\ t \in \mathbb{F}_q \cup \{\infty\}\}$.

Proof. First we identify N with the $\mathbb{F}_q$-rational points of the conic $x^2 + \epsilon^{q+1} y^2 = z^2$. More precisely, if $(x_0 : y_0 : 1)$ is such a point, then we have $\xi = x_0 + \epsilon y_0 \in N$. Now, if we consider the parametrization $t \mapsto (x_t, y_t) = (\frac{t^2+\epsilon^2}{t^2-\epsilon^2}, \frac{2t}{t^2-\epsilon^2})$ of the affine conic, we can endow the elements of N with such a parametrization and write $\xi_t = x_t + \epsilon y_t = \frac{t+\epsilon}{t-\epsilon}$. □

Proposition 4.5. *For every $r \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, there exists $\xi \in N$ such that $\chi_q(1 - (r-\xi)^{q+1}) = 1$.*

Proof. We need to find $\xi \in N$ such that $\chi_q(r^q\xi + r\xi^{-1} - r^{q+1}) = 1$. By Remark 4.4, it suffices to find $t \in \mathbb{F}_q$ such that

$$\begin{aligned}\chi_q\left(\frac{t+\epsilon}{t-\epsilon}r^q + \frac{t-\epsilon}{t+\epsilon}r - r^{q+1}\right) &= \chi_q\left(\frac{(r^q + r - r^{q+1})t^2 + 2\epsilon(r^q - r)t + \epsilon^2(r^q + r + r^{q+1})}{t^2 - \epsilon^2}\right)\\ &= \chi_q\big(\big(t^2-\epsilon^2\big)\big(\big(r^q + r - r^{q+1}\big)t^2 + 2\epsilon\big(r^q - r\big)t + \epsilon^2\big(r^q + r + r^{q+1}\big)\big)\big)\\ &= 1.\end{aligned}$$

Now, it is just a matter of finding a lower bound on the number of $\mathbb{F}_q$-solutions for $u^2 = f(t)$, where

$$f(t) = \big(t^2-\epsilon^2\big)\big(\big(r^q + r - r^{q+1}\big)t^2 + 2\epsilon\big(r^q - r\big)t + \epsilon^2\big(r^q + r + r^{q+1}\big)\big) \in \mathbb{F}_q[t]. \tag{4.2}$$

Note that since $r^q - r \neq 0$, the above equation is not of the form $u^2 = \mu g(t)^2$, where $\chi_q(\mu) = -1$. Therefore, if q is not too small, we can find a solution we need. In fact, if $f(t)$ has repeated roots, we can replace the above equation by a conic's equation. If the roots are all distinct, we will have an elliptic curve, and using the Hasse–Weil bound ($|N - (q+1)| \leqslant 2q^{1/2}$), we find $q > 9$ provides a solution we need. Finally, a quick computer check reveals that such fact also holds true for $q \leqslant 9$. □

Corollary 4.6. *If $\chi_{q^2}(r) = -1$ and $s \in N_1$, then there exist b and c in $\mathbb{F}_{q^2}^{\star}$ satisfying the following*:

1. $r - b^2 s = c$.
2. $b^{q+1} = 1$.
3. $\chi_q(1 - c^{q+1}) = 1$.

Proof. Since we have $\chi_{q^2}(r/s) = -1$, by Proposition 4.5, there exists $\xi' \in N$ such that $\chi_q(1 - (r/s - \xi')^{q+1}) = 1$. On the other hand, because of Lemma 4.3, we may assume $\xi' \in N_2$, which implies $\xi' = \xi^2$

for some $\xi \in N$. Therefore, we have $\chi_q(1-(r/s-\xi^2)^{q+1}) = \chi_q(1-(r-\xi^2 s)^{q+1}) = 1$. Now, taking $b = \xi$ and $c = r - \xi^2 s$, we get the result. □

Proof of Theorem 4.1. Let $P = (x_0 : y_0 : z_0) \in PG(2, q^2)$ be a point in the complement of Γ. If one of its coordinates is zero, for instance $z_0 = 0$, then we take the line $z = 0$ which clearly intersects $\Gamma(\mathbb{F}_{q^2})$ in $d = (q+1)/2$ distinct points. Suppose the point is given by $P = (x_0 : y_0 : 1)$ with $x_0 y_0 \neq 0$, and consider the following possibilities:

- $\chi_{q^2}(x_0) = 1$ or $\chi_{q^2}(y_0) = 1$.

Without loss of generality, we assume $\chi_{q^2}(y_0) = 1$, and since $y_0^{(q+1)/2} \in \mathbb{F}_q$, the line $y = y_0 z$ intersects Γ in d distinct points, unless $y_0^{(q+1)/2} = -1$. On the other hand, if we also have $\chi_{q^2}(x_0) = 1$, then this problem can be fixed by taking either the line $x = x_0 z$ or $x = \frac{x_0}{y_0} y$. Thus, we only need to consider the case $y_0^{(q+1)/2} = \chi_{q^2}(x_0) = -1$.

- $\chi_{q^2}(x_0) = \chi_{q^2}(y_0) = -1$.

Since $P = (x_0 : y_0 : 1) = (1 : \frac{y_0}{x_0} : \frac{1}{x_0})$, using the symmetry of the curve, one can see that we fall on the previous case.

Based on this, we may assume that $P = (r : s : 1)$ with r, s satisfying $\chi_{q^2}(r) = s^{(q+1)/2} = -1$.

We take the values b and c provided by Corollary 4.6, and consider the line l containing P and given by $x - b^2 y = cz$. In order to prove that l is incident with $(q+1)/2$ distinct points of $\Gamma(\mathbb{F}_{q^2})$, it suffices to prove that the conic $\mathcal{C}$: $x^2 - b^2 y^2 = cz^2$ intersects the Hermitian curve $\mathcal{H}$: $x^{q+1} + y^{q+1} + z^{q+1} = 0$ in $2(q+1)$ distinct points $P = (x : y : 1) \in PG(2, q^2)$. One can check that $(t : u) \mapsto (bct^2 + bu^2 : ct^2 - u^2 : 2btu)$ parametrizes $\mathcal{C}$, and that the intersection restricted to the affine points of both curves yields

$$b^{q+1}\left(ct^2+1\right)^{q+1} + \left(ct^2-1\right)^{q+1} + 4b^{q+1}t^{q+1} = 0.$$

Since $b^{q+1} = 1$, we have

$$c^{q+1}t^{2(q+1)} + 2t^{q+1} + 1 = 0. \tag{4.3}$$

For $\Delta = 4(1 - c^{q+1})$, Corollary 4.6(3) gives us $\chi_q(\Delta) = 1$, which implies that (4.3) has $2(q+1)$ distinct non-zero roots in $\mathbb{F}_{q^2}$. Since this gives $2(q+1)$ affine points of $(\mathcal{H} \cap C)(\mathbb{F}_{q^2})$, the result follows. □

In the previous computation, we noted a way to find conics not intersecting the Hermitian curve in $PG(2, q^2)$. Also, it is well known that the intersection of these curves with lines in $PG(2, q^2)$ can be easily characterized. These two facts will be the tools to prove Theorem 4.2.

Proof of Theorem 4.2. Since $q > 3$, we can find $c \in \mathbb{F}_{q^2}^{\star}$ such that $\chi_q(1 - c^{2(q+1)}) = -1$, and we claim the conic $\mathcal{C}$: $x^2 - y^2 = (cz)^2$ does not intersect the Hermitian curve $\mathcal{H}$: $x^{q+1} + y^{q+1} + z^{q+1} = 0$ in $PG(2, q^2)$. In fact, considering the same parametrization used in the proof of Theorem 4.1, one can check that we end up with the following:

$$c^{2(q+1)}t^{2(q+1)} + 2t^{q+1} + 1 = 0. \tag{4.4}$$

For $\Delta = 4(1 - c^{2(q+1)})$, we have $\chi_q(\Delta) = -1$, which implies $\mathcal{C}$ intersects $\mathcal{H}$ in $2(q+1)$ points defined over a non-trivial extension of $\mathbb{F}_{q^2}$. Now, Bezout's theorem implies our claim.

For the arc property, we consider a point $P \in PG(2, q^2)$ in the complement of the two curves. Among the q^2+1 lines incident with P, we know that there are $q+1$ lines tangent to $\mathcal{H}$, and each of the remaining q^2-q lines intersects the Hermitian curve in $q+1$ distinct points (see Theorem 1.2). On the other hand, we also know that there are at most $(q^2+3)/2$ lines through P which are not secant to $\mathcal{C}$. Therefore, if we have $q^2-q > (q^2+3)/2$, which means $q > 3$, then the (N, d)-arc is complete. □

5. A Fermat curve

Here, we obtain a small complete (N, d)-arc in $PG(2, q^2)$ given by the $\mathbb{F}_{q^2}$-rational points of the Fermat curve $\mathcal{C}$: $x^{q-1} + y^{q-1} + z^{q-1} = 0$. In [10], Moisio presents an explicit formula for the number of $\mathbb{F}_{q^2}$-rational points of a certain family of Fermat curves. It turns out that $\mathcal{C}$ lies in this family. However, to make our future discussion clearer, the computation of $\mathcal{F}(\mathbb{F}_{q^2})$ is also presented here.

Theorem 5.1. *Let $q \equiv 2 \bmod 3$ be a power of a prime $p > 2$. If $\mathcal{C}$ is the Fermat curve $x^{q-1} + y^{q-1} + z^{q-1} = 0$, then $\#\mathcal{C}(\mathbb{F}_{q^2}) = 2q^2 - q - 1$.*

Proof. It is clear that $\mathcal{C}$ has $3(q-1)$ points in $PG(2, q^2)$ with $xyz = 0$. To count the points with non-zero coordinates, it suffices to count the number of solutions of $x + y + 1 = 0$ for x and y in $\mathcal{N} = \{\xi \in \mathbb{F}_{q^2} \colon \xi^{q+1} = 1\}$.

Recall from Remark 4.4 that if we fix $\epsilon \in \mathbb{F}_{q^2}$, such that $\epsilon^{q-1} = -1$, then we have $\mathcal{N} = \{\frac{t+\epsilon}{t-\epsilon} \colon t \in \mathbb{F}_q \cup \{\infty\}\}$. Since $p \neq 3$, the pairs $(u, v) \in \mathcal{N} \times \mathcal{N}$ with $u + v + 1 = 0$ correspond to the pairs $(t_1, t_2) \in \mathbb{F}_q \times \mathbb{F}_q$ with

$$\frac{t_1+\epsilon}{t_1-\epsilon} + \frac{t_2+\epsilon}{t_2-\epsilon} + 1 = 0$$

and thus

$$3t_1t_2 - \epsilon(t_1 + t_2) - \epsilon^2 = 0. \tag{5.1}$$

Since $\epsilon \notin \mathbb{F}_q$, (5.1) gives $t_1 = -t_2$ and $\epsilon^2 = -3t_1^2$. Note that $\epsilon^2 = -3t_1^2$ is consistent only if -3 is a non-square in $\mathbb{F}_q$, which turns out to be equivalent to $3 \mid (q+1)$. From $t_1 = -t_2$ we have $1 + u + u^2 = 0$, i.e. u is a primitive cubic root of unity. Therefore, (u, u^{-1}) and (u^{-1}, u) are the only solutions of $x + y + 1 = 0$ for x and y in $\mathcal{N}$ (such characterization will be important in the proof of Theorem 5.2).

Clearly, each solution above gives rise to $(q-1)^2$ points in $\mathcal{C}(\mathbb{F}_{q^2})$ with non-zero coordinates. Hence, we have $\#\mathcal{C}(\mathbb{F}_{q^2}) = 2(q-1)^2 + 3(q-1) = 2q^2 - q - 1$. □

Theorem 5.2. *Let q be an odd prime power such that $3 \mid (q+1)$. If $\mathcal{C}$ is the Fermat curve $x^{q-1} + y^{q-1} + z^{q-1} = 0$, then $\#\mathcal{C}(\mathbb{F}_{q^2})$ is a complete $(2q^2 - q - 1, q - 1)$-arc.*

Proof. Let $P = (x_0 : y_0 : z_0) \in PG(2, q^2)$ be a point in the complement of $\mathcal{C}$. If one of the coordinates of P is zero, say $z_0 = 0$, then the line $z = 0$ obviously contains P and intersects $\mathcal{C}$ in $q-1$ distinct points of $PG(2, q^2)$. Therefore, we can assume $P = (r : s : 1)$ with $rs \neq 0$. The following claim excludes several more possibilities for $P = (r : s : 1)$.

Claim I. *Let μ be a fixed element of $\mathbb{F}_{q^2}$ satisfying $\mu^{2(q-1)} + \mu^{q-1} + 1 = 0$. If $r, s \in \mathbb{F}_{q^2}^{\star}$ such that $\{\mu r/s, \mu^2/s, \mu/r\} \cap \mathbb{F}_q \neq \emptyset$, then there exists a line l incident with $P = (r : s : 1)$ with $\#(l \cap \mathcal{C}(\mathbb{F}_{q^2})) = q - 1$.*

Proof. Suppose we have $\mu r/s = \alpha \in \mathbb{F}_q$ and consider the line l: $x = (r/s)y$. Clearly $P \in l$, and since $1 + \mu^{q-1} + \mu^{2(q-1)} = 0$, the polynomial $((\alpha/\mu)y)^{q-1} + y^{q-1} + 1$ has $q-1$ distinct roots in $\mathbb{F}_{q^2}$ which implies $\#(l \cap \mathcal{C}(\mathbb{F}_{q^2})) = q-1$. The other two cases can be handled in an identical way if we consider the lines $y = sz$ and $x = rz$, respectively. □

From now on, we will use the same fixed μ defined in Claim I and assume $r, s \in \mathbb{F}_{q^2}^{\star}$ do not satisfy the hypotheses of that claim. To deal with the remaining cases, we will prove the existence of $\lambda \in \mathbb{F}_{q^2}$ such that the polynomial $f(x) = x^{q-1} + (\lambda(x-r)+s)^{q-1} + 1$ has $q-1$ distinct zeros in $\mathbb{F}_{q^2}$. Suppose $f(x)$ has a zero $x_0 \in \mathbb{F}_{q^2}$ corresponding to an $\mathbb{F}_{q^2}$-rational point of $\mathcal{C}$ with non-zero coordinates. Based on such points of $\mathcal{C}$ (characterized in Theorem 5.1), we can find x_1 and y_1 in $\mathbb{F}_{q^2}^{\star}$ such that one of the following holds:

1. $x_0 = \mu x_1^{q+1}$ and $\lambda(x_0 - r) + s = \mu^2 y_1^{q+1}$, and thus $\lambda(\mu x_1^{q+1} - r) + s = \mu^2 y_1^{q+1}$.
2. $x_0 = \mu^2 x_1^{q+1}$ and $\lambda(x_0 - r) + s = \mu y_1^{q+1}$, and thus $\lambda(\mu^2 x_1^{q+1} - r) + s = \mu y_1^{q+1}$.

Note that in each case, such a zero of $f(x)$ gives rise to $(q+1)^2$ $\mathbb{F}_{q^2}$-rational solutions (with non-zero coordinates) of the equations given by

$$\lambda\mu X^{q+1} - \mu^2 Y^{q+1} + s - \lambda r = 0 \tag{5.2}$$

and

$$\lambda\mu^2 X^{q+1} - \mu Y^{q+1} + s - \lambda r = 0, \tag{5.3}$$

respectively. Conversely, we can also see that such $(q+1)^2$ solutions for (5.2) or (5.3) give rise to a unique zero of $f(x)$.

Now, the idea is to find $\lambda \in \mathbb{F}_{q^2}$ such that either (5.2) or (5.3) has the maximum possible number of $\mathbb{F}_{q^2}$-solutions. This will be achieved if the coefficients of either equation can be replaced by elements of $\mathbb{F}_q^{\times}$.

Claim II. *There exist m, n in $\mathbb{F}_q^{\times}$ such that $s - \mu r m = \mu^2 n$.*

Proof. Since $s, \mu r, \mu^2 \in \mathbb{F}_{q^2}^{\star}$, we can certainly find $\alpha_1, \alpha_2, \alpha_3$ in $\mathbb{F}_q$, not all zero, such that

$$\alpha_1 s + \alpha_2 \mu r + \alpha_3 \mu^2 = 0.$$

On the other hand, it is easy to check that if $\alpha_i = 0$ for some $i \in \{1, 2, 3\}$, then r, s will satisfy the hypotheses of Claim I, violating our assumption. Finally, defining $m = -\alpha_2/\alpha_1$ and $n = -\alpha_3/\alpha_1$ completes the proof. □

Using the previous claim, we take $\lambda = \mu m$, and after some scaling (if necessary), (5.2) and (5.3) can be replaced by

$$X^{q+1} + Y^{q+1} + 1 = 0 \tag{5.4}$$

and

$$\mu X^{q+1} + \mu^2 Y^{q+1} + 1 = 0. \tag{5.5}$$

Table 1
Complete (N, d)-arcs

	d	$q = p^m$ odd	N	$N - G \leqslant$
1	$q-3$	$p > 5$	$q^2 - 5q + 6$	1
2	$q-5$	$p > 5$	$q^2 - 8q + 15$	2
3	$q-7$	$3 \mid (q-1)$ and $p > 5$	$q^2 - 11q + 37$	3
4	$q-9$	$4 \mid (q-1)$ and $p > 5$	$q^2 - 14q + 45$	4
5	$q-13$	$6 \mid (q-1)$ and $p > 7$	$q^2 - 20q + 91$	6
6	$q - p^h$	$h \mid m$ and $p > 5$	$\frac{2q^2-(3p^h+1)q+p^{2h}+p^h}{2}$	$\frac{p^r-1}{2}$
7	$q - 4p^h + 3$	m/h is even and $p > 5$	$q^2 + (4 - 6p^h)q + 8p^{2h} - 10p^h + 3$	$2(p^h - 1)$
8	$\sqrt{q} + 3$	$q > 9$ square	$q\sqrt{q} + q + 2$	1
9	$(q-1)/2$	$q > 11$	$(q^2 + 4q - 5)/4$	$\lceil (q-11)/4 \rceil$
10	$(q+3)/2$	q	$(q^2 + 4q + 7)/4$	$\lceil (q-3)/4 \rceil$
11	$(\sqrt{q}+1)/2$	q square	$(q\sqrt{q} + 3\sqrt{q} + 4)/4$	$\lceil (\sqrt{q}-5)/4 \rceil$
12	$\sqrt{q} - 1$	q square and $3 \mid (\sqrt{q}+1)$	$2q - \sqrt{q} - 1$	$\sqrt{q} - 4$

Lastly, counting the number of $\mathbb{F}_{q^2}$-solutions with non-zero coordinates of the above equations, one can check that the $(q-2)(q+1)^2$ solutions of (5.4) together with the $(q+1)^2$ solutions of (5.5) provide $(q-2)+1 = q-1$ distinct roots for $f(x)$. Hence, we have a complete $(2q^2 - q - 1, q - 1)$-arc. □

6. The parameters

Here, we present a table summarizing our (N, d)-arcs and briefly compare some of our parameters with others previously obtained. We also provide an upper bound on the distance of the corresponding codes to the Griesmer bound.

A linear $[N, k, r]$-code over $\mathbb{F}_q$ is a subspace W of rank k of the vector space $\mathbb{F}_q^N$ in which every non-zero vector in W has at least r non-zero coordinates and some vector in W has exactly r non-zero coordinates. The Griesmer bound [9, Theorem 5.2.6] states that

$$N \geqslant \sum_{i=0}^{k-1} \left\lceil \frac{r}{q^i} \right\rceil =: G.$$

For $r = N - d$, it is well known that linear $[N, 3, r]$-codes over $\mathbb{F}_q$ and (N, d)-arcs in $PG(2, q)$ are equivalent objects. For a more detailed discussion on this correspondence we refer to [1] and [2].

It turns out that an (N, d)-arc in $PG(2, q)$, with $N > (d-2)q + d$, is equivalent to a code meeting the Griesmer bound. Table 1 of [2] lists many of the known families of such (N, d)-arcs, and, more recently, Ball and Montanucci (see [1]) presented new $[N, 3, N-d]$-codes over $\mathbb{F}_q$, with $d = q-3$ and $d = q-4$, meeting the Griesmer bound. Despite the given examples, constructing codes meeting the Griesmer bound is a difficult problem. Actually, obtaining (N, d)-arcs with N/q large, say $N/q > d-2$, is not easy in general. As mentioned in Section 5 of [2], the best that can be done in general is to take (a) for $d < q/2$ the union of $\lfloor d/2 \rfloor$ conics, which gives $N/q > d/2$, and (b) for $d > q/2$ large the complement of the union of $2(q-d)+1$ lines of a dual $(2(q-d)+1, 2)$-arc, which gives $N/q > q - 2d + (2d^2 - d)/q$.

After comparing parameters, we see the (N, d)-arcs obtained from our work here are smaller than the ones from Table 1 of [2], and in general larger than the ones obtained from the above procedures. For instance, each (N, d)-arc derived from Theorem 2.2 satisfies $N/q > d - \alpha$ for some constant $\alpha \geqslant 2$. To give a better idea of the general scenario, we present a table that displays the parameters of the (N, d)-arcs constructed in the previous sections. The last column shows an upper bound for the difference of N and the Griesmer bound (G) of the corresponding $[N, 3, N-d]$-code.

Note that for $d = (q-1)/2$ the (N, d)-arc from procedure (a) above and the one from row 9 in Table 1 give similar values for N. On the other hand, after a careful analysis of the configuration of

our points (Theorem 3.1), we see that such a set can never be given by a union of conics. This leads us to suspect that the (N, d)-arcs will not be the same in general.

It is also worth noting that, in contrast with the other cases in Table 1, row 12 presents a very small (N, d)-arc. We have $N/q < 2$, and as far as we know, there is no construction of arcs with similar parameters.

Table 1 above also shows that, in general, the codes corresponding to our (N, d)-arcs will not meet the Griesmer bound. However, in many cases, they are just a constant away from this bound. It can be checked that, with the exception of rows 6 and 7, the numbers on the last column are the actual value of $N - G$ if q is sufficiently large.

For another comparison, we point out that Ball and Montanucci (see [1]) also presented a (non-explicit) construction of (N, d)-arcs where, under certain conditions, the corresponding codes are one away from the Griesmer bound. It can be checked that the (N, d)-arcs from rows 1 and 8 in Table 1 are not particular cases of this construction. In the case of row 1, we have a smaller value for N. In the case of row 8, our (N, d)-arc does not have the parameters satisfying the required conditions of their construction.

We have noticed that, out of the explicit constructions of (N', d')-arcs in $PG(2, q)$ where the parameter d' matches with our d, our N has a different value and, in some cases, it is slightly smaller. This means we indeed have new parameters. Of course, we are not including the cases where q is too small.

We end this section by presenting three particular cases where some of our (N, d)-arcs ($d \geqslant 4$) have the corresponding codes meeting the Griesmer bound. The notation $[N, d]_q$ will stand for an (N, d)-arc in $PG(2, q)$. Such arcs are: $[20, 4]_7$, $[63, 6]_{13}$ and $[32, 4]_{13}$, and they are obtained from rows 1, 3 and 4, respectively. We have not seen such (N, d)-arcs listed in the most recently updated tables.

Acknowledgments

The author would like to thank Professor Voloch for his many valuable comments and suggestions during the course of this project and the referees for their careful reading of the original manuscript.

References

[1] S. Ball, E. Montanucci, Affine blocking sets, three dimensional codes and the Griesmer bound, Discrete Math. 307 (2007) 1600–1608.
[2] S. Ball, J.W.P. Hirschfeld, Bounds on (n, r)-arcs and their application to linear codes, Finite Fields Appl. 11 (2005) 326–336.
[3] A. Cossidente, J.W.P. Hirschfeld, G. Korchmros, F. Torres, On plane maximal curves, Compos. Math. 121 (2000) 163–181.
[4] A. Garcia, H. Stichtenoth, C.P. Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2000) 137–170.
[5] A. Garcia, J.F. Voloch, Fermat curves over finite fields, J. Number Theory 30 (1988) 345–356.
[6] M. Giullietti, F. Pambianco, F. Torres, E. Ughi, On complete arcs arising from plane curves, Des. Codes Cryptogr. 25 (2002) 237–246.
[7] A. Hefez, J.F. Voloch, Frobenius non classical curves, Arch. Math. 54 (1990) 263–273.
[8] J.W.P. Hirschfeld, Projective Geometry over Finite Fields, second ed., Oxford Univ. Press, Oxford, 1998.
[9] J.H. van Lint, An Introduction to Coding Theory, third ed., Springer, Berlin, 1988.
[10] M. Moisio, On the number of rational points on some families of Fermat curves over finite fields, Finite Fields Appl. 13 (2007) 546–562.
[11] R. Pardini, Some remarks on plane curves over fields of finite characteristic, Compos. Math. 60 (1986) 3–17.
[12] F. Rodriguez Villegas, J.F. Voloch, D. Zagier, Construction of plane curves with many points, Acta Arith. 99 (2001) 85–96.
[13] K.-O. Stöhr, J.F. Voloch, Weierstrass points and curves over finite fields, Proc. London Math. Soc. (3) 52 (1986) 1–19.
[14] J.F. Voloch, A note on (k, n)-arcs, Discrete Math. 294 (2005) 223–224.